

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

Overview

Plaintiff accuses Defendant of infringement through making, using, selling, offering for sale, and importation of Zoho's ("Defendant" or "Zoho") ManageEngine, including Endpoint Central and Vulnerability Manager Plus (the "Accused System and Method"), and all substantially similar products. The term "Accused System and Method" includes the associated computer hardware, interfaces, software, and data, and the processes and methods related thereto.

The Accused System and Method is accused of directly infringing U.S. Patent No. 10,075,466 (the "'466 Patent"). Plaintiff further accuses Defendant of indirectly infringing the '466 Patent by providing its customers and others the Accused System and Method to utilize in an infringing manner. Defendant intends to cause infringement by its customers and users as Defendant instructs users to use the Accused System and Method in an infringing manner. Defendant deploys client software to implement the Accused System and Method. Defendant also provides support and implementation services for the Accused System and Method, including providing instructions, guides, online materials, and technical support.

The asserted claims include elements that are implemented, at least in part, by proprietary electronics and software in the Accused System and Method. The precise designs, processes, and algorithms used in them are held secret, at least in part, and are not publicly available in their entirety. An analysis of Defendant's documentation and/or source code may be necessary to fully and accurately describe all infringing features and functionality of the Accused System and, accordingly, Plaintiff reserves the right to supplement these contentions once such information is made available to Plaintiff. Furthermore, Plaintiff reserves the right to revise these contentions, including as discovery in the case progresses, in view of the Court's final claim construction in this action and in connection with the provision of its expert reports.

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho**

10,075,466 Claim 1	Evidence
<p>An apparatus, comprising: an intrusion prevention node configured to:</p>	<p>ManageEngine <i>an intrusion prevention node configured to</i> (e.g., The vulnerability information collected across multiple endpoints that are connected to the server)</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Intrusion detection and prevention</p> <div data-bbox="600 634 1864 727" style="border: 1px solid red; padding: 5px;"> <p>Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of</p> </div> <p>privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.</p> <p>At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.</p> <p>https://www.manageengine.com/security.html?meseach</p>

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho













	<div><div>See what matters most at a glimpse with dashboard widgets</div><div><div>The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.</div><div>These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.</div></div><div><div><div>Vulnerability Severity Summary</div><div>Zero-day vulnerabilities</div><div>Vulnerability Age Matrix</div><div>Vulnerabilities Over Time</div><div>High Priority Vulnerabilities</div></div><div><div>High Priority Vulnerabilities: Where your primary focus should be!</div><div><div><div>Vulnerabilities</div><div>Vulnerable Software</div><div>View More</div></div><div><table><tr><th>Vulnerabilities</th><th>Affected Systems</th><th>Exploit Status</th><th>Software Name</th></tr><tr><td> Security Update for Windows 8.1 for x64-based Systems (KB3010788)</td><td>1</td><td>Available</td><td>Windows 8.1 Enterprise Edition (x64)</td></tr><tr><td> Security Update for Windows 8.1 for x64-based Systems (KB3010788)</td><td>1</td><td>Available</td><td>Windows 8.1 Home Basic Edition (x64)</td></tr><tr><td> Security Update for Windows 8.1 for x64-based Systems (KB3010788)</td><td>1</td><td>Available</td><td>Windows 8.1 Home Premium Edition (x64)</td></tr><tr><td> Security Update for Windows 8.1 for x64-based Systems (KB3010788)</td><td>1</td><td>Available</td><td>Windows 8.1 Professional Edition (x64)</td></tr></table></div></div><div><div>Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your vulnerability assessment process.</div><div>https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html</div></div></div></div></div>	Vulnerabilities	Affected Systems	Exploit Status	Software Name	 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)	 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)	 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)	 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)
Vulnerabilities	Affected Systems	Exploit Status	Software Name																		
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)																		
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)																		
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)																		
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)																		
receive a result of at least one operation performed on at least one of a plurality of	<div>ManageEngine receive a result of at least one operation performed on at least one of a plurality of networked devices (e.g., The vulnerability information collected by scanning operation) the at least one operation based on first information from at least one first data storage identifying a plurality of</div>																				

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho**

<p>networked devices, the at least one operation based on first information from at least one first data storage identifying a plurality of potential vulnerabilities including at least one first potential vulnerability and at least one second potential vulnerability, the at least one operation configured for:</p>	<p><i>potential vulnerabilities</i> (e.g., emerging vulnerabilities) <i>including at least one first potential vulnerability and at least one second potential vulnerability</i> (e.g., Multiple vulnerability information collected from open source and stored in central database after verification and then system scan across multiple endpoints)</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <div data-bbox="594 565 1864 734" style="border: 2px solid red; padding: 5px;"> <p>Intrusion detection and prevention</p> <p>Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of</p> </div> <p>privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.</p> <p>At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.</p> <p>https://www.manageengine.com/security.html?mesearch</p>
--	--

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

Comprehensive vulnerability scanning

Eliminating blind spots is the basis of successful **vulnerability management**. To achieve this, Vulnerability Manager Plus:

- Detects known or emerging vulnerabilities across all your network endpoints, including workstations, laptops, servers, web servers, databases, virtual machines, and content management systems.
- Offers continuous visibility into your endpoints, whether they are located at the local office, in a demilitarized zone, at a remote location, or always on the move.
- Extends your visibility beyond just vulnerabilities and identifies misconfigurations, high-risk software, active ports, and much more.

<https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html>

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho****Leverage a dedicated view for zero-days**

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.

The screenshot displays the ManageEngine Vulnerability Manager Plus dashboard. The left sidebar shows a navigation menu with options like 'Threats', 'Software Vulnerabilities', 'Zero-day Vulnerabilities', 'System Misconfigurations', 'High Risk Software', 'Web Server Misconfiguration', and 'Port Audit'. The main content area is titled 'Threats' and includes a sub-header: 'This view displays zero day vulnerabilities like Wannacry, Meltdown and Spectre, etc. that are present in your network.' Below this, there is a filter section with 'Filter by: Threat Category' and a search bar 'Search by CVE ID: CVE-XXXX-XXXX'. A table lists several vulnerabilities, including Google Chrome (x64) (78.0.3904.87) and various Internet Explorer security updates. The table columns are 'Threats', 'Threat Category', 'Affected Systems', and 'Action'. The 'Action' column contains a 'Fix' link for each entry. At the bottom right of the table, it shows '1 - 5 of 5' and a '30' dropdown menu.

Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network.

Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. [Subscribe](#) to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news

<https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html>

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

Vulnerability Manager Plus Server:

The Vulnerability Manager Plus Server helps you to centrally perform all the vulnerability management and compliance tasks in your network endpoints. Some of the tasks include the following:

- Installing agents in computers
- Scanning computers for vulnerabilities and misconfigurations
- Deploying patches and secure configurations
- Uninstalling high-risk software
- Auditing active ports
- Auditing for compliance against CIS benchmarks

Any of the Windows computers in your network with the requirements mentioned [here](#) can be hosted as your Vulnerability Manager Plus Server. This Vulnerability Manager Plus Server at the customer site subscribes to the Central Vulnerability Database, from which it synchronizes the latest information on threats, patches, vulnerabilities, and compliance policies. Patches are downloaded directly from vendor sites and stored centrally in the server's patch store and will be replicated to your network endpoints to conserve bandwidth.

<https://www.manageengine.com/vulnerability-management/help/vulnerability-management-architecture.html#v1>

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho**

	<div><div>See what matters most at a glimpse with dashboard widgets</div><div>The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results. These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.</div><div><div>Vulnerability Severity Summary</div><div>Zero-day vulnerabilities</div><div>Vulnerability Age Matrix</div><div>Vulnerabilities Over Time</div><div>High Priority Vulnerabilities</div></div><div><div>High Priority Vulnerabilities: Where your primary focus should be!</div><div><div><div>Vulnerabilities</div><div>Vulnerable Software</div><div>View More</div></div><table><thead><tr><th>Vulnerabilities</th><th>Affected Systems</th><th>Exploit Status</th><th>Software Name</th></tr></thead><tbody><tr><td> Security Update for Windows 8.1 for x64-based Systems (KB3010788)</td><td>1</td><td>Available</td><td>Windows 8.1 Enterprise Edition (x64)</td></tr><tr><td> Security Update for Windows 8.1 for x64-based Systems (KB3010788)</td><td>1</td><td>Available</td><td>Windows 8.1 Home Basic Edition (x64)</td></tr><tr><td> Security Update for Windows 8.1 for x64-based Systems (KB3010788)</td><td>1</td><td>Available</td><td>Windows 8.1 Home Premium Edition (x64)</td></tr><tr><td> Security Update for Windows 8.1 for x64-based Systems (KB3010788)</td><td>1</td><td>Available</td><td>Windows 8.1 Professional Edition (x64)</td></tr></tbody></table></div><div><p>Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your vulnerability assessment process.</p><p>https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html</p></div></div></div>	Vulnerabilities	Affected Systems	Exploit Status	Software Name	Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)	Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)	Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)	Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)
Vulnerabilities	Affected Systems	Exploit Status	Software Name																		
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)																		
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)																		
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)																		
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)																		
identifying at least one configuration associated with	ManageEngine identifying at least one configuration associated with the at least one networked device (e.g., The vulnerability information collected by scanning operation and identify a misconfiguration).																				

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

<p>the at least one networked device, and</p>	<p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>How to prevent security misconfigurations?</p> <hr/> <p>If vulnerabilities are the gateway to the network, it's the misconfigurations that attackers leverage to worm their way to the intended targets. Security misconfigurations are not hard to fix, but they are unavoidable in an enterprise operating at scale. Finding them is a needle in the haystack, as they can be located across any component in an organization's systems, such as its servers, operating systems, applications, and browsers. Lack of visibility and centralized means to remediate misconfigurations makes organizations fall victim to misconfiguration attacks.</p> <p>https://www.manageengine.com/vulnerability-management/misconfiguration/?meseach</p>
---	---

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho**

	<p>As soon as it's up and running in your network, Vulnerability Manager Plus automatically discovers your Active Directory and workgroup assets. Scaling up? No problem. Since Vulnerability Manager Plus is constantly in sync with Active Directory, new assets will be brought under management as soon as they enter your network, leaving no opportunity for new threats to go unnoticed.</p> <p>Leveraging endpoint agent technology, Vulnerability Manager Plus scans your laptops, desktops, servers, databases, workstations, and virtual machines across your entire global hybrid IT environment every 90 minutes, irrespective of whether they're within the corporate boundary or not.</p> <p>You can set up distribution servers, which replicate primary server commands, for your remote offices simplify management and conserve bandwidth. You can even manage assets within a closed network like a DMZ.</p> <p>Identified systems are probed for different attributes: operating systems, open ports, installed software, user accounts, file system structure, system configurations, and more. Using the library of up-to-date scan data, Vulnerability Manager Plus checks the discovered assets for threats and vulnerabilities and delivers appropriate remediation.</p> <p>https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html</p>
<p>determining that the at least one networked device is actually vulnerable to at least one actual vulnerability, based on the identified at least one configuration and the first information from the</p>	<p>ManageEngine <i>determining that the at least one networked device is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration and the first information from the at least one first data storage identifying the plurality of potential vulnerabilities</i> (e.g., The vulnerability information collected by scanning operation and identify a misconfiguration based on vulnerability information collected from open source and stored in central database). <i>such that second information associated with the result is stored in at least one second data storage separate from the at least one first data storage</i> (e.g., The vulnerability information collected across multiple endpoints is consolidated in a</p>

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho**

at least one first data storage identifying the plurality of potential vulnerabilities, such that second information associated with the result is stored in at least one second data storage separate from the at least one first data storage, the second information relating to the at least one actual vulnerability to which the at least one networked device is actually vulnerable;

web console for centralized management which is different from central database). *the second information relating to the at least one actual vulnerability to which the at least one networked device is actually vulnerable* (e.g., The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and if vulnerabilities exist then displays them in a dedicated view in the console with its fix)

Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

How to prevent security misconfigurations?



If vulnerabilities are the gateway to the network, it's the misconfigurations that attackers leverage to worm their way to the intended targets. Security misconfigurations are not hard to fix, but they are unavoidable in an enterprise operating at scale. Finding them is a needle in the haystack, as they can be located across any component in an organization's systems, such as its servers, operating systems, applications, and browsers. Lack of visibility and centralized means to remediate misconfigurations makes organizations fall victim to misconfiguration attacks.

<https://www.manageengine.com/vulnerability-management/misconfiguration/?mesearch>

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho**

See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity
Summary


Zero-day
vulnerabilities

Vulnerability
Age Matrix

Vulnerabilities
Over Time

**High Priority
Vulnerabilities**

High Priority Vulnerabilities: Where your primary focus should be!

Vulnerabilities		Vulnerable Software			
Vulnerabilities		Affected Systems	Exploit Status	Software Name	
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	1	Available	Windows 8.1 Enterprise Edition (x64)	
				Windows 8.1 Home Basic Edition (x64)	
				Windows 8.1 Home Premium Edition (x64)	
				Windows 8.1 Professional Edition (x64)	

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho****Leverage a dedicated view for zero-days**

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.

The screenshot shows the ManageEngine Vulnerability Manager Plus interface. The left sidebar contains a navigation menu with options: Threats, Software Vulnerabilities, Zero-day Vulnerabilities, System Misconfigurations, High Risk Software, Web Server, Misconfiguration, Port Audit, and Update Vulnerability DB. The main content area is titled 'Threats' and includes a description: 'This view displays zero day vulnerabilities like Wannacry, Meltdown and Spectre, etc. that are present in your network.' Below this is a filter section with 'Filter by: Threat Categ...' and a search bar 'Search by CVE ID: CVE-XXXX-XXXX'. A table displays the following data:

Threats	Threat Category	Affected Systems	Action
Google Chrome (x64) (78.0.3904.87)	ZeroDay_CVE-2019-13721&_CVE-2019-...	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675&CVE-2019-1255	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675&CVE-2019-1255	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...	IE_ZeroDay_CVE-2018-8653	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	IE_ZeroDay_CVE-2018-8653	1	Fix

At the bottom right of the table, it shows '1 - 5 of 5' and a pagination control '30'.

Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network. Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. [Subscribe](#) to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news

<https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html>

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

| How can I view the complete list of CVEs affecting my endpoints?

Vulnerability Manager Plus boasts a dedicated Detected CVEs view that lists all the CVEs affecting your network endpoints. All you have to do is select the desired CVEs then click Fix CVE to instantly create a patch deployment task in all the affected machines.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

As soon as it's up and running in your network, Vulnerability Manager Plus automatically discovers your Active Directory and workgroup assets. Scaling up? No problem. Since Vulnerability Manager Plus is constantly in sync with Active

Directory, new assets will be brought under management as soon as they enter your network, leaving no opportunity for new threats to go unnoticed.

Leveraging endpoint agent technology, Vulnerability Manager Plus scans your laptops, desktops, servers, databases, workstations, and virtual machines across your entire global hybrid IT environment every 90 minutes, irrespective of whether they're within the corporate boundary or not.

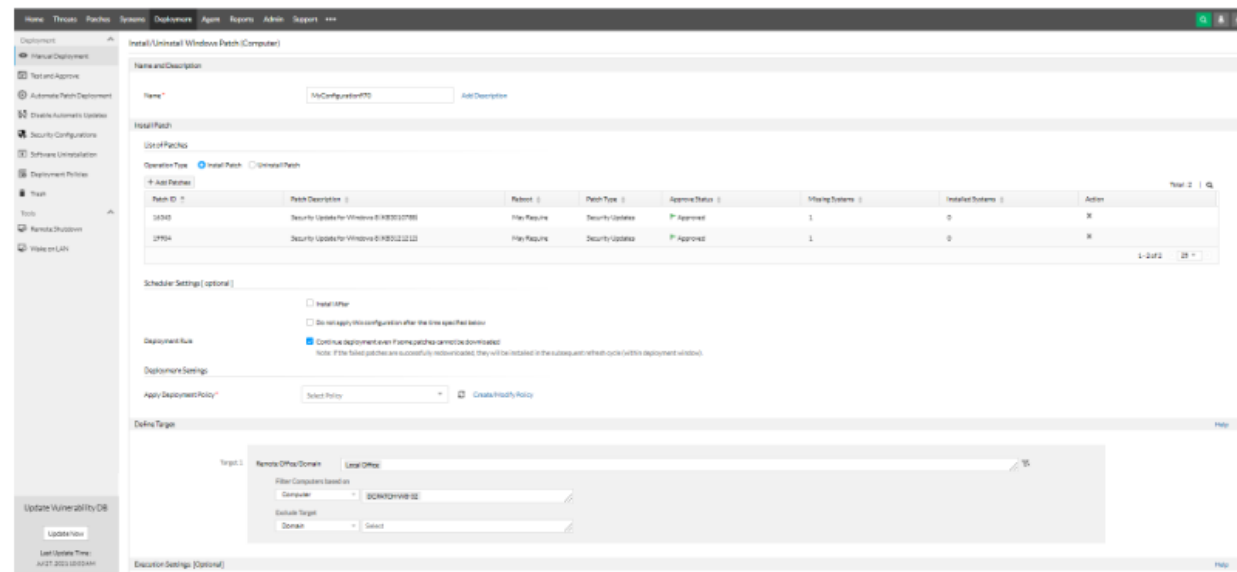
You can set up distribution servers, which replicate primary server commands, for your remote offices simplify management and conserve bandwidth. You can even manage assets within a closed network like a DMZ.

Identified systems are probed for different attributes: operating systems, open ports, installed software, user accounts, file system structure, system configurations, and more. Using the library of up-to-date scan data, Vulnerability Manager Plus checks the discovered assets for threats and vulnerabilities and delivers appropriate remediation.

<https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html>

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.



<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

cause display, via at least one user interface, a plurality of

ManageEngine *causes to display, via at least one user interface* (e.g., ManageEngine Vulnerability Manager Plus includes web console) , *a plurality of techniques including a first technique for utilizing an*

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho**

techniques including a first technique for utilizing an intrusion prevention system component for occurrence mitigation, and a second technique for utilizing a firewall for occurrence mitigation;

intrusion prevention system component for occurrence mitigation (e.g., ManageEngine Vulnerability Manager Plus includes antivirus option), and a second technique for utilizing a firewall for occurrence mitigation (e.g., ManageEngine Vulnerability Manager Plus includes firewall option). The ManageEngine provides flexibility to choose the devices for applying the different policies or mitigation techniques according to the requirements.

Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

Intrusion detection and prevention

Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of

privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.

At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.

<https://www.manageengine.com/security.html?meseach>

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho**

Security Configuration Management with ManageEngine Vulnerability Manager Plus

ManageEngine Vulnerability Manager Plus License Version: 10.0.621

Home Threats Patches Systems Deployment Reports Agent Admin Support

This view displays all the inappropriately configured security settings in your Windows systems.

Filter by: Severity Category

Total: 62

Description	Category	Affected Systems	Severity
Geolocation is enabled to track user location	Windows Firewall	2	Info
TLSv1.1 protocol is enabled	SSL and TLS Security	1	Info
Administrative Shares enabled	Share Permission Management	3	Info
Data Execution Prevention is not enabled	Chrome Security Hardening	4	Critical
Maximum Password age is not configured to 45 days	Password Policy	1	Critical
Secure logon (Ctrl+Alt+Delete logon) is not enabled	Logon Security	1	Critical
Antivirus (not considering Windows Defender) not installed	Antivirus Protection	1	Critical
Account lockout duration is not configured to 1440 minutes	Logon Security	2	Critical
Built-in Administrator Account is not disabled	User Account Management	2	Critical
Folder shares are assigned to everyone group	Share Permission Management	2	Critical
Windows firewall disabled/ No third-party firewall present	Windows Firewall	1	Critical
Outdated plugins are allowed to run	Chrome Security Hardening	2	Critical

Update Vulnerability DB

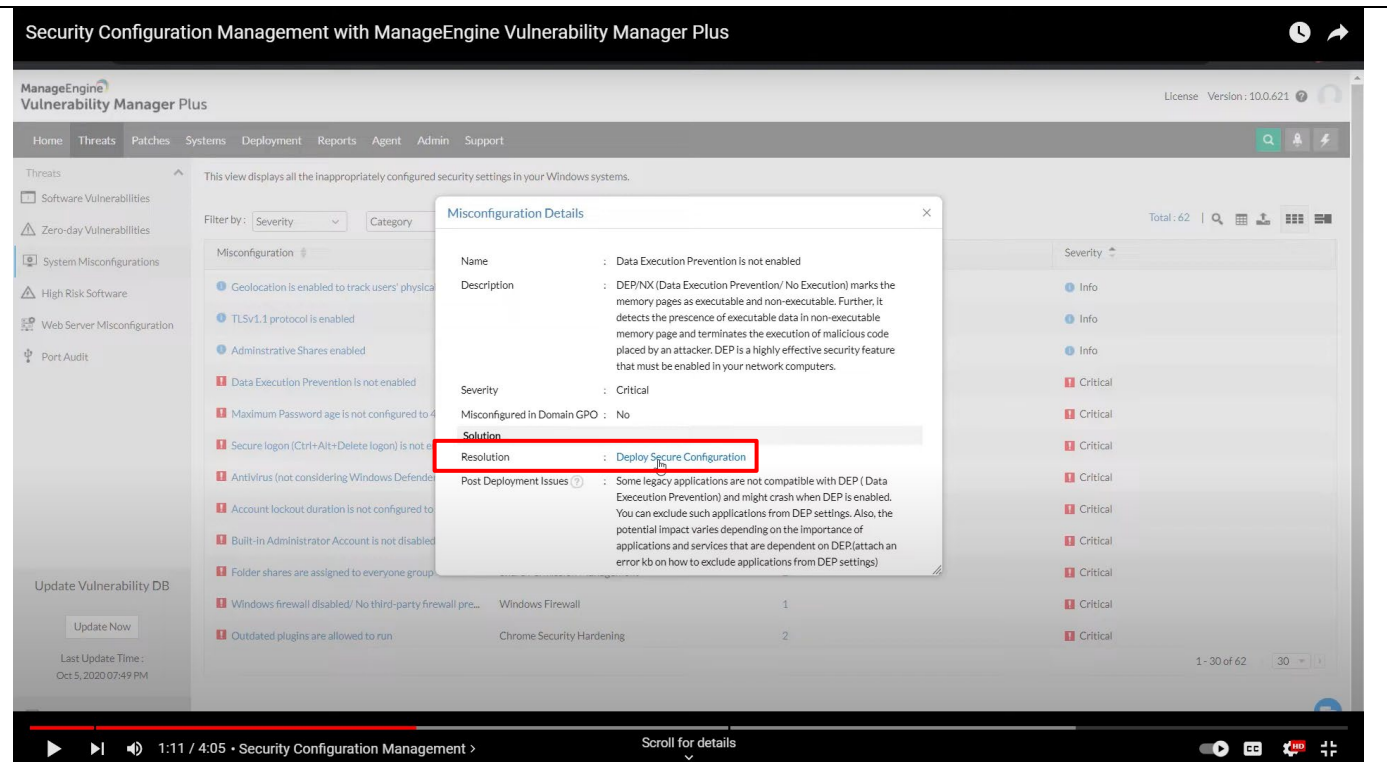
Update Now

MORE VIDEOS

1:39 / 4:05 - Security Configuration Management

YouTube

<https://www.youtube.com/watch?v=p2Oh87NruMo&t=98s>

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho**

<https://www.youtube.com/watch?v=p20h87NruMo&t=53s>

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

Firewall Policy Management

Firewall Analyzer is a firewall administration software, that helps in administering firewall rules and policies into multiple firewalls. The firewall rule automation ensures that firewall rules are pushed into the device seamlessly, avoiding errors and oversight. This firewall administration tool is capable of making the following changes.

- Add, modify, and delete network and service objects
- Add, modify, and delete firewall rules
- Analyze the implications of proposed firewall rule changes
- Push changes directly to the firewall

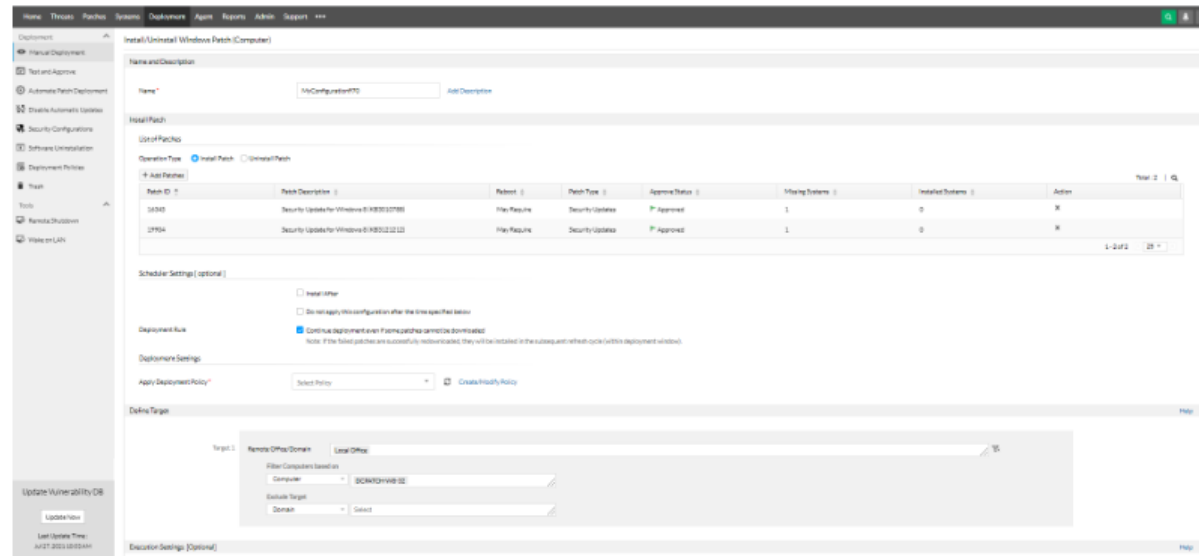
Refer the 'Firewall Rule Administration' page for more details.

Firewall Analyzer is an efficient firewall rule and policy management tool that helps you gain visibility on all firewall rules, optimize firewall rules, and remove rule anomalies. It provides rule management reports for [most major firewall devices](#) including [Cisco](#), [FortiGate](#), [WatchGuard](#), and [Check Point](#).

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.



<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

allows receipt of:

ManageEngine allows receipt, user input causing selection of the first technique for utilizing the intrusion prevention system component for occurrence mitigation (e.g., ManageEngine Vulnerability Manager Plus

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho**

<p>user input causing selection of the first technique for utilizing the intrusion prevention system component for occurrence mitigation;</p> <p>user input causing selection of the second technique for utilizing the firewall for occurrence mitigation;</p>	<p>includes web consol on which user can select antivirus option) , <i>user input causing selection of the second technique for utilizing the firewall for occurrence mitigation</i> (e.g., ManageEngine Vulnerability Manager Plus includes firewall option). The ManageEngine provides flexibility to choose the devices for applying the different policies or mitigation techniques according to the requirements.</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Intrusion detection and prevention</p> <p>Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.</p> <p>At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.</p> <p>https://www.manageengine.com/security.html?mesearch</p>
---	--

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho**

The screenshot displays the ManageEngine Vulnerability Manager Plus interface. The left sidebar shows navigation options: Threats, Software Vulnerabilities, Zero-day Vulnerabilities, System Misconfigurations (selected), High Risk Software, Web Server Misconfiguration, and Port Audit. The main content area shows a list of system misconfigurations. A dropdown menu for 'Category' is open, showing options: Antivirus Protection, User Account Management, Windows Firewall, Password Policy, SSL and TLS Security, and Chrome Security Hardening. A red box highlights a list of critical misconfigurations, including 'Secure logon (Ctrl+Alt+Delete logon) is not enabled', 'Antivirus (not considering Windows Defender) not installed', 'Account lockout duration is not configured to 1440 minutes', 'Built-in Administrator Account is not disabled', 'Folder shares are assigned to everyone group', and 'Windows firewall disabled/ No third-party firewall present'. The interface also includes filters for Severity and Category, a table of affected systems, and a 'Total: 62' count.

Misconfiguration	Category	Affected Systems	Severity
Secure logon (Ctrl+Alt+Delete logon) is not enabled	Logon Security	1	Critical
Antivirus (not considering Windows Defender) not installed	Antivirus Protection	1	Critical
Account lockout duration is not configured to 1440 minutes	Logon Security	2	Critical
Built-in Administrator Account is not disabled	User Account Management	2	Critical
Folder shares are assigned to everyone group	Share Permission Management	2	Critical
Windows firewall disabled/ No third-party firewall present	Windows Firewall	1	Critical

<https://www.youtube.com/watch?v=p2Oh87NruMo&t=98s>

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho**

The screenshot displays the ManageEngine Vulnerability Manager Plus interface. A modal window titled "Misconfiguration Details" is open, showing the following information:

- Name:** Data Execution Prevention is not enabled
- Description:** DEP/NX (Data Execution Prevention/ No Execution) marks the memory pages as executable and non-executable. Further, it detects the presence of executable data in non-executable memory page and terminates the execution of malicious code placed by an attacker. DEP is a highly effective security feature that must be enabled in your network computers.
- Severity:** Critical
- Misconfigured in Domain GPO:** No
- Solution:** (Section header)
- Resolution:** Deploy Secure Configuration (This line is highlighted with a red box)
- Post Deployment Issues:** Some legacy applications are not compatible with DEP (Data Execution Prevention) and might crash when DEP is enabled. You can exclude such applications from DEP settings. Also, the potential impact varies depending on the importance of applications and services that are dependent on DEP (attach an error kb on how to exclude applications from DEP settings)

The background interface shows a list of misconfigurations with filters for Severity and Category. The "Update Vulnerability DB" button is visible at the bottom left of the main panel.

<https://www.youtube.com/watch?v=p20h87NruMo&t=53s>

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

Firewall Policy Management

Firewall Analyzer is a firewall administration software, that helps in administering firewall rules and policies into multiple firewalls. The firewall rule automation ensures that firewall rules are pushed into the device seamlessly, avoiding errors and oversight. This firewall administration tool is capable of making the following changes.

- Add, modify, and delete network and service objects
- Add, modify, and delete firewall rules
- Analyze the implications of proposed firewall rule changes
- Push changes directly to the firewall

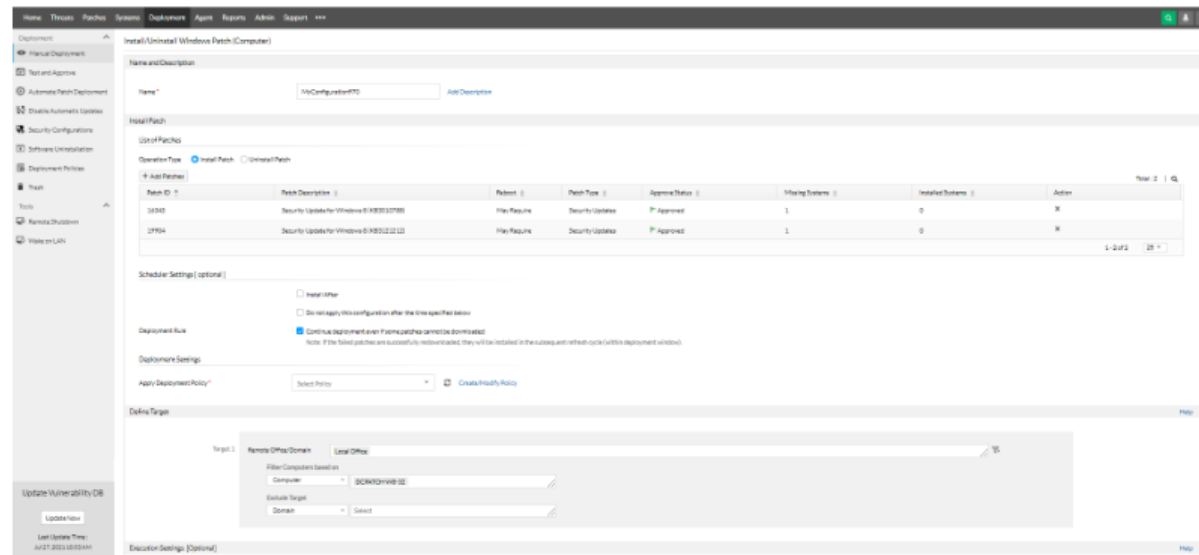
Refer the 'Firewall Rule Administration' page for more details.

Firewall Analyzer is an efficient firewall rule and policy management tool that helps you gain visibility on all firewall rules, optimize firewall rules, and remove rule anomalies. It provides rule management reports for [most major firewall devices](#) including [Cisco](#), [FortiGate](#), [WatchGuard](#), and [Check Point](#).

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.



<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

apply, based on the user input causing selection of the first

ManageEngine apply, based on the user input causing selection of the first technique for utilizing the intrusion prevention system component for occurrence mitigation, the first technique for utilizing the

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho**

technique for utilizing the intrusion prevention system component for occurrence mitigation, the first technique for utilizing the intrusion prevention system component for occurrence mitigation;

apply, based on the user input causing selection of the second technique for utilizing the firewall for occurrence mitigation, the second technique for utilizing the firewall for occurrence mitigation;

intrusion prevention system component for occurrence mitigation (e.g., ManageEngine Vulnerability Manager Plus includes web consol on which user can select antivirus option) , *apply, based on the user input causing selection of the second technique for utilizing the firewall for occurrence mitigation, the second technique for utilizing the firewall for occurrence mitigation* (e.g., ManageEngine Vulnerability Manager Plus includes firewall option). The ManageEngine provides flexibility to choose the devices for applying the different policies or mitigation techniques according to the requirements.

Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

Intrusion detection and prevention

Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of

privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.

At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.

<https://www.manageengine.com/security.html?meseach>

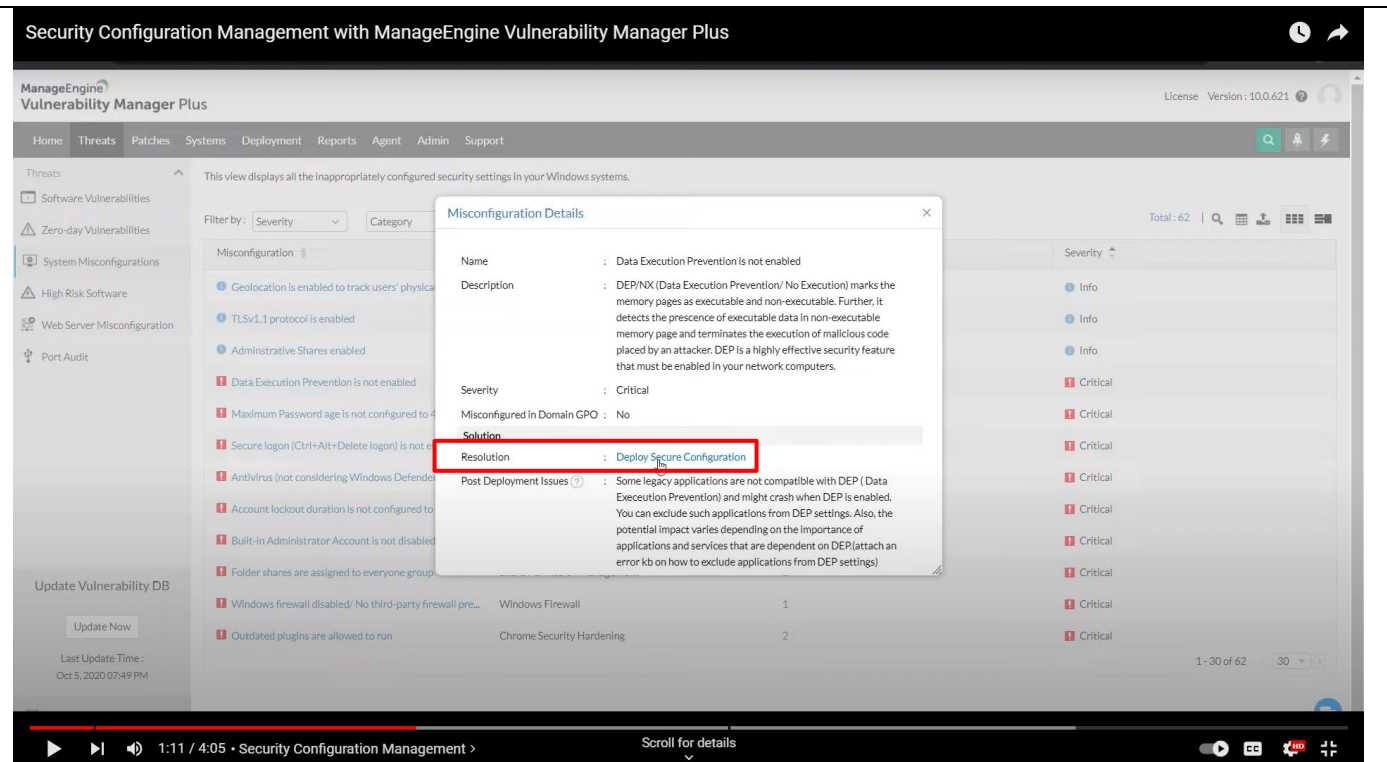
EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho**

The screenshot displays the ManageEngine Vulnerability Manager Plus interface. The left sidebar shows navigation options: Threats, Software Vulnerabilities, Zero-day Vulnerabilities, System Misconfigurations (selected), High Risk Software, Web Server Misconfiguration, and Port Audit. The main content area shows a list of misconfigurations with filters for Severity and Category. A dropdown menu for 'Category' is open, showing options: Antivirus Protection, User Account Management, Windows Firewall, Password Policy, SSL and TLS Security, and Chrome Security Hardening. A red box highlights a list of critical misconfigurations:

Misconfiguration	Category	Affected Systems	Severity
Secure logon (Ctrl+Alt+Delete logon) is not enabled	Logon Security	1	Critical
Antivirus (not considering Windows Defender) not installed	Antivirus Protection	1	Critical
Account lockout duration is not configured to 1440 minutes	Logon Security	2	Critical
Built-in Administrator Account is not disabled	User Account Management	2	Critical
Folder shares are assigned to everyone group	Share Permission Management	2	Critical
Windows firewall disabled/ No third-party firewall present	Windows Firewall	1	Critical

The interface also includes a 'Update Vulnerability DB' button and a 'MORE VIDEOS' link. The bottom of the screenshot shows a YouTube video player interface with the title 'Security Configuration Management' and a progress bar at 1:39 / 4:05.

<https://www.youtube.com/watch?v=p2Oh87NruMo&t=98s>

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho**

<https://www.youtube.com/watch?v=p20h87NruMo&t=53s>

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

Firewall Policy Management

Firewall Analyzer is a firewall administration software, that helps in administering firewall rules and policies into multiple firewalls. The firewall rule automation ensures that firewall rules are pushed into the device seamlessly, avoiding errors and oversight. This firewall administration tool is capable of making the following changes.

- Add, modify, and delete network and service objects
- Add, modify, and delete firewall rules
- Analyze the implications of proposed firewall rule changes
- Push changes directly to the firewall

Refer the 'Firewall Rule Administration' page for more details.

Firewall Analyzer is an efficient firewall rule and policy management tool that helps you gain visibility on all firewall rules, optimize firewall rules, and remove rule anomalies. It provides rule management reports for [most major firewall devices](#) including [Cisco](#), [FortiGate](#), [WatchGuard](#), and [Check Point](#).

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.

The screenshot displays the 'Install Patch' configuration page in the ManageEngine Vulnerability Management console. The page is titled 'Install (Universal) Windows Patch (Computer)' and includes a sidebar with navigation options like 'Home', 'Threats', 'Patches', 'Systems', 'Deployment', 'Agent', 'Reports', 'Admin', and 'Support'.

Name and Description: The 'Name' field is set to 'MSConfiguredP02'.

Install Patch: The 'Operation Type' is set to 'Install Patch'.

Table of Patches:

Patch ID	Patch Description	Reboot	Patch Type	Approval Status	Missing Systems	Installed Systems	Action
10300	Security Update for Windows 8.1 KB3033708	Not Required	Security Update	Approved	1	0	X
10304	Security Update for Windows 8.1 KB3033712	Not Required	Security Update	Approved	1	0	X

Scheduler Settings (optional): Includes options for 'Install on first boot' and 'Do not apply this configuration after the time specified below'.

Deployment Rule: A checkbox labeled 'Continue deployment even if some patches are not installed' is checked.

Deployment Settings: The 'Apply Deployment Policy' dropdown is set to 'Select Policy'.

Define Target: The 'Target' is set to 'Remote Office/Domain' and 'Local Office'. The 'Filter Computers based on' dropdown is set to 'Computer' with the value 'BOWTOWARD-02'.

Execution Settings (Optional): A section for additional configuration options.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

<p>identify :</p> <p>for the at least one networked device, a first occurrence including at least one first occurrence packet, and</p> <p>for the at least one networked device, a second occurrence including at least one second occurrence packet;</p>	<p>ManageEngine <i>identify, for the at least one networked device, a first occurrence including at least one first occurrence packet (e.g., Bad traffic), for the at least one networked device, a second occurrence including at least one second occurrence packet (e.g., good traffic).</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>DDoS prevention</p> <p>We use technologies from well-established and trustworthy service providers to prevent DDoS attacks on our servers. These technologies offer multiple DDoS mitigation capabilities to prevent disruptions caused by bad traffic, while allowing good traffic through. This keeps our websites, applications, and APIs highly available and performing.</p> <p>https://www.manageengine.com/security.html?meseach</p>
---	--

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho**

	<p>Intrusion detection and prevention</p> <p>Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents.</p> <p>At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.</p> <p>At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.</p> <p>https://www.manageengine.com/security.html?mesearch</p>
<p>determine:</p> <p>that the first occurrence including the at least one first occurrence packet directed to the at least one networked device is capable of taking advantage of the at least one</p>	<p>ManageEngine <i>determine, that the first occurrence including the at least one first occurrence packet directed to the at least one networked device is capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable (e.g., Bad traffic) , that the second occurrence including the at least one second occurrence packet directed to the at least one networked device is not capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable (e.g., good traffic).</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p>

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho**

of the actual vulnerability to which the at least one networked device is actually vulnerable;

that the second occurrence including the at least one second occurrence packet directed to the at least one networked device is not capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable; and

DDoS prevention

We use technologies from well-established and trustworthy service providers to prevent DDoS attacks on our servers. These technologies offer multiple DDoS mitigation capabilities to prevent disruptions caused by bad traffic, while allowing good traffic through. This keeps our websites, applications, and APIs highly available and performing.

<https://www.manageengine.com/security.html?mesearch>

Intrusion detection and prevention

Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents.

At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.

At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.

<https://www.manageengine.com/security.html?mesearch>

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

<p>cause a reporting of at least the first occurrence based on the determination that the first occurrence including the at least one first occurrence packet directed to the at least one networked device is capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable.</p>	<p>ManageEngine <i>cause a reporting of at least the first occurrence based on the determination that the first occurrence including the at least one first occurrence packet directed to the at least one networked device is capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable</i> (e.g., mitigation capabilities to prevent disruptions caused by bad traffic and reported to the user)</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>DDoS prevention</p> <p>We use technologies from well-established and trustworthy service providers to prevent DDoS attacks on our servers. These technologies offer multiple DDoS mitigation capabilities to prevent disruptions caused by bad traffic, while allowing good traffic through. This keeps our websites, applications, and APIs highly available and performing.</p> <p>https://www.manageengine.com/security.html?mesearch</p>
---	--

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

Intrusion detection and prevention

Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.

At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.

<https://www.manageengine.com/security.html?mesearch>

EXHIBIT 14**U.S. Patent No 10,075,466 v. Zoho****Leverage a dedicated view for zero-days**

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.

The screenshot shows the ManageEngine Vulnerability Manager Plus interface. The left sidebar contains a navigation menu with options: Threats, Software Vulnerabilities, Zero-day Vulnerabilities, System Misconfigurations, High Risk Software, Web Server Misconfiguration, and Port Audit. The main content area is titled 'Threats' and includes a sub-header: 'This view displays zero day vulnerabilities like Wannacry, Meltdown and Spectre, etc. that are present in your network.' Below this, there is a filter bar with 'Filter by: Threat Category' and a search bar 'Search by CVE ID: CVE-10000-10000'. A table displays the following data:

Threats	Threat Category	Affected Systems	Action
Google Chrome (x64) (78.0.3904.87)	ZeroDay_CVE-2019-13721&CVE-2019-...	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675&CVE-2019-1235	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675&CVE-2019-1235	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...	IE_ZeroDay_CVE-2018-8653	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	IE_ZeroDay_CVE-2018-8653	1	Fix

At the bottom right of the table, it shows '1 - 5 of 5' and a dropdown menu set to '30'. Below the table is a button labeled 'Update Vulnerability DB'.

Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network.

Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. *Subscribe to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news*

<https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html>

EXHIBIT 14

U.S. Patent No 10,075,466 v. Zoho

Incident Management

Reporting

We have a dedicated incident management team. We notify you of the incidents in our environment that apply to you, along with suitable actions that you may need to take. We track and close the incidents with appropriate corrective actions. Whenever applicable, we will identify, collect, acquire and provide you with necessary evidence the form of application and audit logs regarding incidents that apply to you. Furthermore, we implement controls to prevent recurrence of similar situations.

We respond to the security or privacy incidents you report to us through incidents@zohocorp.com, with high priority. For general incidents, we will notify users through our blogs, forums, and social media. For incidents specific to an individual user or an organization, we will notify the concerned party through email (using their primary email address of the Organisation administrator registered with us).

<https://www.manageengine.com/security.html?mesearch>